

UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF NEW YORK

USDC SDNY  
DOCUMENT  
ELECTRONICALLY FILED  
DOC #:  
DATE FILED: 3/13/2020

-----X  
WILLIAM GRECIA,

Plaintiff,

-against-

BANK OF NEW YORK MELLON  
CORPORATION,

Defendant.  
-----

WILLIAM GRECIA,

Plaintiff,

-against-

CITIBANK, N.A.,

Defendant.  
-----

WILLIAM GRECIA,

Plaintiff,

-against-

MORGAN STANLEY SMITH BARNEY LLC,

Defendant.  
-----

WILLIAM GRECIA,

Plaintiff,

-against-

TIAA, FSB d/b/a TIAA Bank,

Defendant.  
-----

19-CV-2810 (VEC)  
19-CV-2811 (VEC)  
19-CV-2812 (VEC)  
19-CV-2813 (VEC)  
19-CV-3278 (VEC)

OPINION AND ORDER

-----	:
WILLIAM GRECIA,	:
	:
Plaintiff,	:
	:
-against-	:
	:
SAMSUNG ELECTRONICS AMERICA, INC.,	:
	:
Defendant.	:
-----	X

VALERIE CAPRONI, United States District Judge:

The above-captioned cases all involve claims of patent infringement. Plaintiff William Grecia is the inventor of U.S. Patent No. 8,887,308 (the “’308 Patent”), which relates to digital rights management (“DRM”). Technologies within DRM control and limit user access to digital content. According to Grecia, prior art DRM systems could not authorize access to licensed content across multiple devices, such as a phone, tablet, and computer, but, instead, tethered access rights to a particular device. Grecia’s patent includes one claim (“Claim 1”) that teaches a method for transforming a user’s access request into an authorization object that facilitates access across different devices. Each Defendant—four national banks and Samsung Electronics America, Inc.—offers similar online financial applications that Grecia alleges directly infringe upon his patent.

Defendants have moved to dismiss the respective complaints for failure to state a claim under Federal Rule of Civil Procedure 12(b)(6). They argue, *inter alia*, that Claim 1 is patent-ineligible under 35 U.S.C. § 101 and *Alice Corp. v. CLS Bank Int’l*, 573 U.S. 208, 216 (2014). Because the Court agrees, the motions to dismiss are GRANTED.

## BACKGROUND<sup>1</sup>

The '308 Patent is titled “Digital Cloud Access (PDMAS Part III)” and teaches a DRM solution for accessing licensed content across multiple devices. DRM refers to access control technologies that prevent undesirable or illegal use of digital media content, such as internet-delivered music and video files. Am. Compl. Ex. A (hereinafter, “Spec.”) at 1:29–34. The patent’s innovation is to “brand” digital content—*i.e.* write information to the content’s metadata—with information about the user’s identity and right to access that content. *Id.* at 3:1–8, 4:3–10. The branded information travels with the digital content so that a user can access the content from different devices. The '308 Patent concludes with one claim teaching “a process for transforming a user access request for cloud digital content into a computer readable authorization object.” *Id.* at 14:31–33.

On September 8, 2018, Judge Sullivan construed several of Claim 1’s terms.<sup>2</sup> Am. Compl. ¶ 7 (citing Order, *Grecia v. MasterCard Int’l Inc.*, No. 15-CV-9059 (S.D.N.Y. Sept. 8,

---

<sup>1</sup> On this motion to dismiss, the Court accepts all factual allegations in the pleadings as true and draws all reasonable inferences in the light most favorable to Plaintiff. *See Gibbons v. Malone*, 703 F.3d 595, 599 (2d Cir. 2013). The Court may also “consider any written instrument attached to the complaint, statements or documents incorporated into the complaint by reference, legally required public disclosure documents filed with the [Securities and Exchange Commission], and documents possessed by or known to the plaintiff upon which it relied in bringing the suit.” *Tongue v. Sanofi*, 816 F.3d 199, 209 (2d Cir. 2016) (quoting *ATSI Comme’ns, Inc. v. Shaar Fund, Ltd.*, 493 F.3d 87, 98 (2d Cir. 2007)).

The parties have submitted five separate sets of pleadings for each case. These pleadings are identical in all material respects. For purposes of this Opinion, the Court refers to the pleadings filed in the first-listed captioned case, *Grecia v. Bank of N.Y. Mellon Corp.*, as representative of the rest. The Court uses the following abbreviations: Amended Complaint (Dkt. 37) as “Am. Compl.”; Defendant’s Memorandum of Law in Support of Its Motion to Dismiss the Amended Complaint (Dkt. 40) as “Mem. of Law Supp. Mot.”; Opposition to Motion to Dismiss by Plaintiff William Grecia (Dkt. 41) as “Pl.’s Opp.”; Defendant’s Reply in Support of Its Motion to Dismiss the Amended Complaint (Dkt. 42) as “Reply.”

<sup>2</sup> Judge Sullivan did not rule on any of the issues presented here.

2018), Dkt. 89 (hereinafter, “*MasterCard*”)). In the discussion below, this Court further elaborates the steps of Claim 1 and incorporates Judge Sullivan’s constructions into those steps.

Grecia has filed five nearly identical lawsuits against Bank of New York Mellon, Citibank, Morgan Stanley, and TIAA Bank (collectively, the “Banks”) and Samsung Electronics America (“Samsung”). Grecia alleges that Claim 1 is directed to patentable subject matter under Section 101. *Id.* ¶ 11. He recites the United States Patent and Trademark Office’s examination of Patent ’308 and three decisions denying petitions for *inter partes* review, in which the patent was challenged on Section 102 and 103 grounds. *See id.* ¶¶ 12–16 & Exs. B–E. Grecia then alleges that Defendants’ various finance and payment applications directly infringe upon the patented Claim 1.

The Banks’ payment applications, in particular, interface with another application, Zelle, to allow users to send and receive money without having to store or process a payee’s bank account information. *Id.* ¶ 17 & Ex. F. The Banks’ applications do so by first authenticating a user’s email address or telephone number and then connecting with Zelle. *Id.* ¶¶ 20–21. The applications then request and receive query data from Zelle. *Id.* ¶ 22. Finally, the applications create and process “a computer readable authorization object” to process financial transactions. *Id.* ¶ 23.

Samsung’s application, Samsung Pay, similarly “transform[s] . . . a user’s credit card account number into a payment token that may be used to make purchases,” according to Grecia. Am. Compl. (19-CV-3278, Dkt. 27) ¶ 17. When a user downloads the Samsung Pay application and seeks to use it to make a purchase, he or she must enter a credit card account number that is used to verify permission to make purchases. *Id.* ¶ 18. The application then authenticates the user’s credit card number and connects with a “Samsung Token Requestor,” from which it

requests and receives a “tokenized card number.” *Id.* ¶¶ 19–21. As a last step, it writes that number to the data store on the user’s device and cross-references it during any subsequent requests to make a purchase using Samsung Pay. *Id.* ¶ 22.

## **DISCUSSION**

### **I. Standard of Review**

To survive a motion to dismiss under Rule 12(b)(6), “a complaint must allege sufficient facts, taken as true, to state a plausible claim for relief.” *Johnson v. Priceline.com, Inc.*, 711 F.3d 271, 275 (2d Cir. 2013) (citing *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555–56 (2007)). “[A] complaint does not need to contain detailed or elaborate factual allegations, but only allegations sufficient to raise an entitlement to relief above the speculative level.” *Keiler v. Harlequin Enters., Ltd.*, 751 F.3d 64, 70 (2d Cir. 2014) (citation omitted). The Court accepts all factual allegations in the complaint as true and draws all reasonable inferences in the light most favorable to the plaintiff. *See Gibbons v. Malone*, 703 F.3d 595, 599 (2d Cir. 2013). The Court, is not, however, “bound to accept as true a legal conclusion couched as a factual allegation.” *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Twombly*, 550 U.S. at 555).

### **II. The Motions to Dismiss Are Not Premature**

As a threshold matter, Grecia argues that the motions to dismiss are not ripe for resolution because the parties disagree whether the Court must first hold another claim-construction proceeding. *See* Pl.’s Opp. at 1. Grecia’s position has no merit. It is settled law that “[s]ubject matter eligibility under § 101 may be determined at the Rule 12(b)(6) stage of a case.” *ChargePoint, Inc. v. SemaConnect, Inc.*, 920 F.3d 759, 765 (Fed. Cir. 2019) (citing *Aatrix Software, Inc. v. Green Shades Software, Inc.*, 882 F.3d 1121, 1125 (Fed. Cir. 2018)). Although it is error for a district court to decide subject-matter eligibility before addressing a claim

construction dispute, the mere existence of such a dispute is not reason to deny a motion to dismiss. *See MyMail, Ltd. v. ooVoo, LLC*, 934 F.3d 1373, 1380 (Fed. Cir. 2019) (citing *Aatrix*, 882 F.3d at 1125). A district court has at least two other options. It may adopt “the non-moving party’s constructions” or otherwise “resolve the disputes to whatever extent is needed to conduct the § 101 analysis, which may well be less than a full, formal claim construction.” *Aatrix*, 882 F.3d at 1125.

Here, the Court accepts Grecia’s proposed constructions. Although there is a dispute whether additional claim construction *proceedings* are necessary (*i.e.*, whether this Court should rely solely upon the prior constructions in *MasterCard*, *see* Proposed Case Management Plan (19-CV-2813, Dkt. 22-1) at 4), the parties do not dispute the meaning of the claim’s particular terms, let alone dispute terms that bear on whether the claim is directed to patent-eligible subject matter. *See MyMail*, 934 at 1380 (holding that the district court erred by ruling on a Rule 12(c) motion where the parties disputed the construction of a term and the district court did not adopt the non-moving party’s construction). Because the Court adopts Grecia’s alleged constructions, there are “no factual allegations that, taken as true, prevent resolving the eligibility question as a matter of law.” *Aatrix*, 882 F.3d at 1125. The Court now proceeds to resolve that question.

### **III. The ’308 Patent Is Directed to Abstract Subject Matter**

The Supreme Court has set out a two-step inquiry to determine whether a patent claims an abstract idea. *See Alice Corp. v. CLS Bank Int’l*, 573 U.S. 208, 216 (2014); *Mayo Collaborative Servs. v. Prometheus Labs., Inc.*, 566 U.S. 66, 72–73 (2012). First, the court must determine whether the claim at issue is directed to an abstract idea. *Alice*, 566 U.S. at 217. If so, the court must determine whether the claim nonetheless “contains an inventive concept sufficient

to transform the claimed abstract idea into a patent-eligible application.” *Id.* at 221 (quotation omitted).

At step one, courts “look at the focus of the claimed advance over the prior art to determine if the claim’s character as a whole is directed to excluded subject matter.” *Chamberlain Grp., Inc. v. Techtronic Indus. Co.*, 935 F.3d 1341, 1346 (Fed. Cir. 2019) (quoting *Affinity Labs of Tex., LLC v. DIRECTV, LLC*, 838 F.3d 1253, 1257 (Fed. Cir. 2016)). “In cases involving software innovations, this inquiry often turns on whether the claims focus on ‘the specific asserted improvement in computer capabilities or, instead, on a process that qualifies as an abstract idea for which computers are invoked merely as a tool.’” *Ancora Techs., Inc. v. HTC Am., Inc.*, 908 F.3d 1343, 1347 (Fed. Cir. 2018), *as amended* (Nov. 20, 2018) (quoting *Finjan, Inc. v. Blue Coat System, Inc.*, 879 F.3d 1299, 1303 (Fed. Cir. 2018)). Thus, a claimed method involving software is patent eligible if it describes a specific improvement over prior art to computer functionality or recites a means particular to computers that solves a problem in an existing technological process. *See Enfish, LLC v. Microsoft Corp.*, 822 F.3d 1327, 1335 (Fed. Cir. 2016); *Koninklijke KPN N.V. v. Gemalto M2M GmbH*, 942 F.3d 1143, 1149–50 (Fed. Cir. 2019). By contrast, a claim is directed to an abstract idea if it does “not claim a particular way of programming or designing the software to [accomplish the claimed functionality], but instead merely claim[s] the resulting systems.” *Apple, Inc. v. Ameranth, Inc.*, 842 F.3d 1229, 1241 (Fed. Cir. 2016). A claim is also directed to an abstract idea if it is “not directed to a specific improvement in the way computers operate.” *Id.*

At step two, courts search for an inventive concept in the claim. An inventive concept is “some element or combination of elements sufficient to ensure that the claim in practice amounts to ‘significantly more’ than a patent on an ineligible concept.” *DDR Holdings, LLC v.*

*Hotels.com, L.P.*, 773 F.3d 1245, 1255 (Fed. Cir. 2014) (quoting *Alice*, 537 U.S. at 218). The court “consider[s] the elements of each claim both individually and as an ordered combination to determine whether the additional elements transform the nature of the claim into a patent-eligible application.” *Alice*, 537 U.S. at 217 (quotation omitted). When a claim is directed to an abstract idea, it must include “additional features to ensure that the claim is more than a drafting effort designed to monopolize the abstract idea.” *Id.* at 221 (quotation omitted). The claim must “involve more than performance of well-understood, routine, and conventional activities previously known to the industry.” *Aatrix*, 882 F.3d at 1128 (quotation omitted). A claim that contains an inventive concept survives an eligibility challenge under Rule 12(b)(6). *Id.* at 1126–27.

Under both steps of *Alice/Mayo*, Claim 1 of Patent ’308 fails.

#### **A. Step One**

The Court finds that Claim 1 is directed to the abstract idea of storing information about permission and identity for processing access requests. It does not teach how to use those two generic pieces of data to process access requests. Nor does it teach any improvement in computer functionality resulting from its method. Instead, Claim 1 covers any means of storing information reflecting (i) a user’s permission to access digital content and (ii) the user’s identity.

The ’308 Patent’s specification itself suggests that Claim 1 is directed to an abstract solution for a general problem. According to the specification, prior art DRM technologies have tied authorization to access content to a particular device by writing the device’s ID to the content’s metadata. Spec. at 2:2–9. To validate access rights, those technologies cross-reference metadata to a clearinghouse according to pre-set rules. *Id.* Thus, they “rely on content providers to maintain computer servers to receive and send session authorization keys to client computers



with an Internet connection.” *Id.* at 2:55–57. Consequently, those DRM measures “do not offer a way to provide unlimited interoperability between different machines.” *Id.* at 3:1–3. The ’308 Patent asserts that “a solution is needed to give consumers the unlimited interoperability between devices and ‘fair use’ sharing partners for an infinite time frame while protecting commercial digital media from unlicensed distribution to sustain long-term return of investments.” *Id.* at 3:3–8. It then purports to provide that solution: “[a]n object of the present invention is to provide unlimited interoperability of digital media between unlimited machines with management of end-user access to the digital media.” *Id.* at 3:12–14. Although identifying a problem is a start, the specification does not offer a concrete and tangible means for solving the identified problem beyond reciting generic steps, components, and data, evincing an attempt to preempt most, if not all, solutions for interoperability.

Notwithstanding the specification, the Court must give ultimate weight to the method taught in Claim 1. *See ChargePoint*, 920 F.3d at 766 (the specification, although “helpful in illuminating what a claim is directed to . . . must always yield to the claim language in identifying that focus”); *see also Alice*, 573 U.S. at 216 (“the concern that drives” the judicial exceptions to patentability is “one of preemption”).

Claim 1 instructs a six-step “process for transforming a user access request for cloud digital content into a computer readable authorization object.” *Id.* 14:31-33.

First, an apparatus with a database receives a request to access “cloud digital content.”<sup>3</sup> Am. Compl. ¶ 7. The apparatus also receives a write request from a user that includes a verification token (step a). The verification token is “data that represents permission to access

---

<sup>3</sup> As determined in *Mastercard*, “cloud digital content” is just “data capable of being processed by a computer.” *Mastercard* at 11.

digital media or cloud digital content.” *Id.* (quoting *MasterCard* at 15). The apparatus then authenticates the user’s token via a token database (step b).

Next, the apparatus connects through an Application Programmable Interface (“API”) to a second apparatus, comprised of a database and a verified web service (step c). To make that connection, the first apparatus provides a credential that the web service recognizes as permission to exchange data.<sup>4</sup> The first apparatus requests and receives query data from the second apparatus that includes an identifier (steps d and e). Finally, the first apparatus writes the verification data and identifier to its data store, which it can subsequently recognize as access rights to cloud digital content (step f).

Claim 1 reads in full as follows:

- a) receiving an access request for cloud digital content through an apparatus in process with at least one CPU, the access request being a write request to a data store, wherein the data store is at least one of: a memory connected to the at least one CPU; a storage connected to the at least one CPU; and a database connected to the at least one CPU through the Internet; wherein the access request further comprises verification data provided by at least one user, wherein the verification data is recognized by the apparatus as a verification token; then
- b) authenticating the verification token of (a) using a database recognized by the apparatus of (a) as a verification token database; then
- c) establishing an API communication between the apparatus of (a) and a database apparatus, the database apparatus being a different database from the verification token database of (b) wherein the API is related to a verified web service, wherein the verified web service is a part of the database apparatus, wherein establishing the API communication requires a credential assigned to the apparatus of (a), wherein the apparatus assigned credential is recognized as a permission to conduct a data exchange session between the apparatus of (a) and the database apparatus to complete the verification process, wherein the data exchange session is also capable of an exchange of query data, wherein the query data comprises at least one verified web service account identifier; then

---

<sup>4</sup> A verified web services means “a web service that is used to authenticate the identity of a user or device.” Am. Compl. ¶ 7 (quoting *Mastercard* at 12).

d) requesting the query data, from the apparatus of (a), from the API communication data exchange session of (c), wherein the query data request is a request for the at least one verified web service identifier; then

e) receiving the query data requested in (d) from the API communication data exchange session of (c); and

f) creating a computer readable authorization object by writing into the data store of (a) at least one of: the received verification data of (a); and the received query data of (e); wherein the created computer readable authorization object is recognized by the apparatus of (a) as user access rights associated to the cloud digital content, wherein the computer readable authorization object is processed by the apparatus of (a) using a cross-referencing action during subsequent user access requests to determine one or more of a user access permission for the cloud digital content.

Spec. at 14:34–15:14.

To discern Claim 1’s focus, it is useful “to compare claims at issue to those claims already found to be directed to an abstract idea in previous cases.” *Enfish*, 822 F.3d at 1334. Although Claim 1 claims an improved result—interoperable access to digital content across devices—it does not teach a “specific way to improve the functionality of a computer.” *Koninklijke*, 942 F.3d at 1152. Claim 1’s method amounts to storing proof of permission and proof of identity to a data store, full stop. It teaches that an apparatus, App 1, receives a request to access digital content, which includes the user’s permission to access that content. App 1 then authenticates that the user has authority to access the data and requests proof of the user’s identity from App 2. The method concludes when App 1 writes both pieces of information to its database for cross-reference during subsequent sessions.<sup>5</sup> Claim 1 provides no technical

---

<sup>5</sup> Grecia summarizes Claim 1 similarly, albeit with slightly more specific language that he asserts limits his claim: “The ’308 patent’s solution—fully disclosed and taught in claim 1—is to write both the user’s permission to access the digital content and *the user’s membership account information* into a data store to be cross referenced upon subsequent access requests.” Pl.’s Opp. at 3 (emphasis added). Defendants dispute that Grecia’s characterization accurately reflects Claim 1, as Claim 1 does not include the concept of storing “membership account information.” See Reply at 2–3. Neither party is correct. Contrary to Defendants’ position, the claim language references the concept of a “verified web service account identifier,” which Judge Sullivan construed as “a

explanation for how to enable interoperable access beyond storing and referencing two generic types of information. The computer components serve as a mere “conduit.” *In re TLI Commc’ns LLC Patent Litig.*, 823 F.3d 607, 612 (Fed. Cir. 2016).

The differences between the eligible and ineligible patent claims in *Data Engine Technologies LLC v. Google LLC* are instructive. 906 F.3d 999 (Fed. Cir. 2018). The *Data Engine* patent identified a problem with computer spreadsheets—they “provided little or no tools for creating and managing [what-if] scenarios” to test the extremes of assumptions in a spreadsheet model. *Id.* at 1005 (quotation omitted). One of the patent’s claims recited “specific steps detailing the method of navigating through spreadsheet pages within a three-dimensional spreadsheet environment using notebook tabs.” *Id.* at 1008. That claim required displaying a row of spreadsheet page identifiers in the form of notebook tabs along one side of the first spreadsheet page. *Id.* It also required “at least one user-settable identifying character to label the notebook tab” and described “navigating through the various spreadsheet pages through selection of the notebook tabs.” *Id.* The Federal Circuit found that “the notebook tabs are specific structures within the three-dimensional spreadsheet environment that allow a user to avoid the burdensome task of navigating through spreadsheets in separate windows using arbitrary commands.” *Id.* at 1011. Consequently, the court held that the claim was not directed to an abstract idea but rather to “a specific method for navigating through three-dimensional electronic spreadsheets.” *Id.* at 1008.

---

web service that is used to authenticate the identity of a user or device.” Am. Compl. ¶ 7 (quoting *Mastercard* at 12). But that concept is still far more generic than Grecia’s characterization. This dispute, however, is largely academic. Whether the Court construes the term as either party defines it does not affect the Court’s decision.

Another claim in the *Data Engine* patent, by contrast, contained only generic recitations of a method that runs on a computer; not “the specific implementation of a notebook tab interface.” *Id.* at 1012. The claim was comprised of four steps, including: “partitioning [a] plurality of cells into a plurality of two-dimensional cell matrices so that each of the two-dimensional cell matrices can be presented to a user as a spreadsheet page”; “associating each of the cell matrices with a user-settable page identifier”; “creating in a first cell of a first page at least one formula referencing a second cell of a second page said formula including the user-settable page identifier for the second page”; and “storing said first and second pages of the plurality of cell matrices such that they appear to the user as being stored within a single file.” *Id.* at 1011–12. The claim was “not limited to the specific technical solution and improvement in electronic spreadsheet functionality” that made the other claim eligible. *Id.* at 1012. Instead, it covered “any means for identifying electronic spreadsheet pages.” *Id.*

Claim 1 is far more similar to the ineligible *Data Engine* claim than the eligible claim. Like the ineligible claim, Claim 1 is not limited to a specific technical solution in digital rights management. It covers any means for validating a user’s access rights using two generic pieces of information. The *sine qua non* of Claim 1 is two types of information—proof of permission and proof of identity—being stored in a generic data store. And unlike the eligible claim in *Data Engine* (a comparison on which Grecia relies), Claim 1 does not recite any particular improvements in computer technology. To the contrary, Claim 1 shuns any reference to specific computer components, objects, or processes, leaning instead on abstractions like “receiving,” “authenticating,” “data store,” “verification token,” “authorization object,” “CPU,” “API,” and “data exchange session.”

Patent '308's specification does little to rein in the broad preemption proposed by Claim 1. For one, the specification is results-oriented and does not “suggest that the invention involved overcoming some sort of technical difficulty.”<sup>6</sup> *ChargePoint*, 920 F.3d at 768. According to the specification, “the present invention teaches a more personal system of digital rights management which employs electronic ID, as part of a web service membership, to manage access rights across a plurality of devices.” Spec. at 1:24–27. And “[a]n object of the present invention is to provide unlimited interoperability of digital media between unlimited machines with management of end-user access to the digital media.” Spec. at 3:12–14. But the specification does not describe how to implement interoperable access with specific computer components. Although the specification outlines several examples instantiating the method of Claim 1, those examples contain only generic computer parts that carry out routine steps (receiving, authenticating, establishing a communication, requesting, and creating). Claim 1 thus “fails to provide any technical details for the tangible components, but instead predominately describes the [method] in purely functional terms.” *TLI Commc'ns*, 823 F.3d at 612.

Defendants press an analogy to a hall monitor and hall pass which, although not dispositive,<sup>7</sup> illustrates Claim 1's shortcomings. See Mem. of Law Supp. Mot. at 3–4, 8. A related analogy that is somewhat closer would be a military police officer (“MP”) dealing with authorization to access a secure military base. The following table summarizes that analogy:

---

<sup>6</sup> Grecia, in his opposition brief, also articulates a solution-oriented focus for Claim 1, reinforcing the Court's conclusion: “Claim 1 is directed to the solution of free, safe access to cloud digital content, requiring that the user's membership and permission to access the digital content be written to a cloud-based data store.” Pl.'s Opp. at 16.

<sup>7</sup> In *Data Engine*, the Federal Circuit reversed the district court for using a real-world analogy to a notebook to find that a patent was directed to an abstract idea. 906 F.3d at 1011. The aptness of an analogy might be telling, but “[i]t is not enough . . . to merely trace the invention to some real-world analogy. That question is reserved for §§ 102 and 103.” *Id.*

<b>Claim 1</b>	<b>Analogy</b>
(a) an apparatus receives a request to access digital content; the request includes a verification token provided by a user.	An MP at the gate of a secure military facility receives a request from a soldier to enter the facility; the soldier shows a military ID.
(b) the apparatus authenticates the verification token.	The MP authenticates the ID.
(c) the apparatus establishes an API communication with a second apparatus.	The MP calls an operator at headquarters.
(d) the apparatus requests query data including a verified web service account identifier through the communication session.	The MP requests information from the operator whether the soldier has orders for that facility.
(e) the apparatus receives the query data.	The MP receives confirmation from the operator that the soldier has been ordered to that facility and provides an authorization number corresponding to the order.
(f) the apparatus creates an authorization object by writing the verification token and identification.	The MP writes into a log the soldier's name from his ID and his authorization number from the operator.

What this analogy demonstrates is that humans can implement the exact process Claim 1 describes without any reference to or reliance upon computers.<sup>8</sup> Claim 1's limitation is nothing more than an abstract and conventional idea applied to computers.

Even assuming the specification is “full of technical details” referencing computer components, the claim it leads to does not require such details. *ChargePoint*, 920 F.3d at 769. Like the patent in *ChargePoint*, Patent '308 is not “intended to improve those particular components,” and nor does Grecia “view[] the combination of those components as [his] invention.” 920 F.3d at 772. Grecia had the idea of storing authorization tokens in a database for cross-device access and retrieval, but Patent '308 goes no further than that. Similarly, in

---

<sup>8</sup> The Court notes that that the hall pass analogy proposed by Defendants was not 100% applicable because it assumed that the student is both the user and the second apparatus and because a hall pass does not typically represent repeat access. The Court's analogy is closer because the MP must communicate both with the soldier, to get his ID, and with an operator, to confirm that the soldier has orders to report to that facility. Moreover, in the Court's analogy, the MP's log book can be used to allow repeated access to the facility. In short, contrary to Grecia's argument, Claim 1 has absolute parallels in the pre-DRM age. See Pl.'s Opp. at 19.

*Ultramercial*, the claims merely recited the abstract idea of “offering media content in exchange for viewing an advertisement,” along with “routine additional steps such as updating an activity log, requiring a request from the consumer to view the ad, restrictions on public access, and use of the Internet.” *Ultramercial, Inc. v. Hulu, LLC*, 772 F.3d 709, 715–16 (Fed. Cir. 2014); *see also SAP Am., Inc. v. InvestPic, LLC*, 898 F.3d 1161, 1163 (Fed. Cir. 2018) (finding that the claims “fit into the familiar class of claims that do not focus on an improvement in computers as tools, but on certain independently abstract ideas that use computers as tools” (quoting *Elec. Power Grp., LLC v. Alstom S.A.*, 830 F.3d 1350, 1354 (Fed. Cir. 2016))).

The claim here is also similar to the claims held to be ineligible in *Uniloc USA, Inc. v. Amazon.com, Inc.*, 243 S. Supp. 3d 797 (E.D. Tex. 2017), *aff’d*, 733 F. App’x 1026 (Fed. Cir. 2018). The claims in that case were a system and method for managing and implementing a time-adjustable license that controlled access to digital content. *Id.* at 800. The claims recited steps such as “*receiving* a request for authorization to use the digital product on a given device” and “*verifying* that a license data associated with the digital product is valid.” *Id.* at 801 (emphasis added). The *Uniloc* court found that the claims were not directed to specific improvements in the functioning of a computer. *Id.* at 804. The claims were instead directed to the abstract idea of time-adjustable licenses and applied that idea to computers for controlling access to licensed software. *Id.* at 804. Similarly, Claim 1 uses generic computer components to control access to digital content through a series of functionally-oriented steps employing conventional computer components. *See also Joao Bock Transaction Sys., LLC v. Jack Henry & Assocs., Inc.*, 76 F. Supp. 3d 513, 522 (D. Del. 2014), *aff’d*, 803 F.3d 667 (Fed. Cir. 2015) (finding that claims merely applied “a conventional business practice utilized by bankers or financial institutions” to computers).



Grecia relies heavily on the prosecution history during which patent examiners rejected three challenges to the '308 patent under 35 U.S.C. §§ 102 and 103. But “it [is not] enough for subject-matter eligibility that claimed techniques be novel and nonobvious in light of prior art, passing muster under 35 U.S.C. §§ 102 and 103.” *SAP*, 898 F.3d at 1163. Grecia’s reliance on the prosecution history betrays that he could not identify a single case with comparable patent claims found eligible under Section 101.

The improvements over prior art in the cases on which Grecia relies involved specific improvements to a computer’s functionality involving particular components. The claim upheld in *Ancora* taught, for example, storing the record of a license for downloaded software in the BIOS memory, rather than other memory. 908 F.3d at 1345. Likewise, the claims in *Visual Memory LLC v. NVIDIA Corp.*, 867 F.3d 1253 (Fed. Cir. 2017), were “directed to a technological improvement: an enhanced computer memory system.” *Id.* at 1259-60. Those claims focused on a “‘specific asserted improvement in computer capabilities’—the use of programmable operational characteristics that are configurable based on the type of processor—instead of ‘on a process that qualifies as an “abstract idea” for which computers are invoked merely as a tool.’” *Id.* (quoting *Enfish*, 822 F.3d at 1336). And, similarly, in *DDR Holdings*, “the claimed solution [was] necessarily rooted in computer technology in order to overcome a problem specifically arising in the realm of computer networks.” 773 F.3d at 1257; *see also Koninklijke*, 942 F.3d at 1153 (holding that claims were eligible because they recited how a data permutation “is used (*i.e.*, modifying the permutation applied to different data blocks), and this specific implementation is a key insight to enabling prior art error detection systems to catch previously undetectable systematic errors”).

In short, the claims in the cases upon which Grecia relies “were patent-eligible because they were directed to improvements in the way computers and networks carry out their basic functions.” *SAP*, 898 F.3d at 1168 (citations omitted). The combination of Claim 1’s steps, by contrast, recites an abstraction with no concrete form.

## **B. Step Two**

Proceeding to *Alice/Mayo* step two, the Court finds that the ’308 Patent does not contain an inventive concept sufficient to transform the claimed abstract idea into a patent-eligible application. The technological components or processes invoked in Claim 1 are not integral to the method’s applications. Claim 1’s reference to an “authorization object,” for example, is just a “‘computer aided limitation’ to a claim covering an abstract concept,” that, “without more, is insufficient to render the claim patent eligible.” *Dealertrack, Inc. v. Huber*, 674 F.3d 1315, 1333 (Fed. Cir. 2012) (quoting *SiRF Tech., Inc. v. Int’l Trade Comm’n*, 601 F.3d 1319, 1333 (Fed. Cir. 2010)). As the MP-access-to-a-secure-facility analogy illustrates, creating the “authorization object” is nothing more than writing down information about permission and identity.<sup>9</sup>

Grecia is not able to identify an inventive concept apart from the abstract idea to which Claim 1 is directed. According to Grecia, Claim 1’s inventive concept is “writing the verified web service account identifier into the data store.” Pl.’s Opp. at 19–20 (citing Am. Compl. ¶¶ 6–7, 11–27). That concept does not qualify as inventive for one fatal reason: it is no different from Claim 1’s ineligible concept of storing information about permission and identity for processing access requests. *See BSG Tech LLC v. Buyseasons, Inc.*, 899 F.3d 1281, 1290 (Fed. Cir. 2018)

---

<sup>9</sup> Claim 1’s invocation of the “cloud” and the “Internet” also does not supply an inventive concept. Merely appealing to the Internet as a channel for the claimed method does not save a patent from ineligibility at the second step of *Alice*. *See Ultramercial*, 772 F.3d at 715 (“Adding routine additional steps . . . and use of the Internet does not transform an otherwise abstract idea into patent-eligible subject matter.”).


(“It has been clear since *Alice* that a claimed invention’s use of the ineligible concept to which it is directed cannot supply the inventive concept that renders the invention ‘significantly more’ than that ineligible concept.”). Grecia effectively concedes that the “only possible inventive concept in [Claim 1] is the abstract idea itself,” *ChargePoint*, 920 F.3d at 775, when he argues that step two of the analysis is “unnecessary [and] redundant because Claim 1’s solution is also the ‘inventive concept’ required to pass step two.” Pl.’s Opp. at 16. Grecia thus conflates Claim 1’s solution—the abstract idea of storing information about permission and identity for processing access requests—with its purported inventive concept.<sup>10</sup>

### CONCLUSION

For the foregoing reasons, Defendants’ motions are GRANTED. Grecia’s complaints are dismissed with prejudice without leave to amend.

The Clerk of Court is respectfully directed to close all captioned cases and open motions.

**Date: March 13, 2020**  
**New York, New York**

  
\_\_\_\_\_  
**VALERIE CAPRONI**  
**United States District Judge**

---

<sup>10</sup> Because the ’308 Patent’s claim is ineligible, these cases must be dismissed. Accordingly, the Court does not address Defendants’ alternative argument that Grecia has not alleged that their applications perform all the steps of Grecia’s claimed method. *See* Mem. of Law Supp. Mot. at 17.